ABSTRACT

Internet allow user to share information through web applications. All information is easily obtained from existing web applications. Web application are currently being targeted by hackers. There are many threats that often attack on web applications. one of them is SQL injection, cross-site scripting, etc. SQL injection is a hacking act performed on a client's application by modifying SQL commands on a client's memory application.

Security on a web application is getting less attention from developers and consequently many attack occured on the web via the Interne. Hence a special security application of the web application firewall with the shadow tools daemon are needed. The web application firewall (waf) is a method for securing the web application on internet.

There are so many that carry out information attacks such as SQL injection threats, cross-site scripting and command injection. An example is the case of the General Election Commission (KPU) website being hacked by hackers from Yogyakarta in 2004, using SQL Injection the hacker managed to change the appearance of the website with very strange information. Therefore, security is needed on web application firewall applications with shadow daemon tools. In this final project, a prototype firewall will be built with ubuntu-based shadow daemon tools on a web server. To secure the web server from attacks on SQL Injections, Cross-Site Scripting, and Command Injection.

Keywords: Waf, Shadow Daemon, SQL Injections, Cross-Site Scripting, Command Injection.